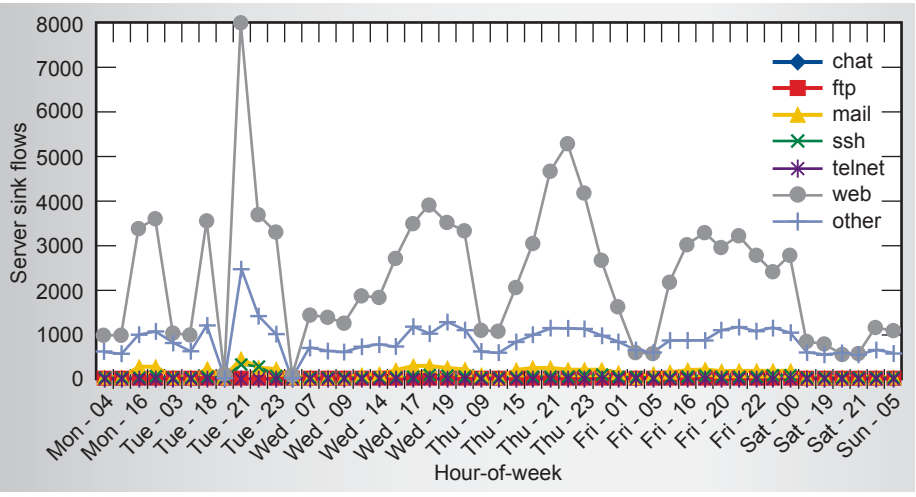
Insider Threat Scenarios and Signatures

Deborah W. May
(925) 422-1448
may14@llnl.gov

Current cyber and information security methods rely on static signature-based approaches to detect and block undesirable network traffic. This is typically done at the perimeter of an intranet or subnet. This approach is extremely limited, especially in a world where malware and adversaries modify their techniques frequently to evade signature-based detection, and perform their malicious functions *within* intranets and on hosts, all distributed across time and IP-space.

To remove some of these limitations, the community is moving toward behavioral signatures that evolve over time. Additionally, rather than addressing network security at a single point, such as the firewall, there is increasing interest in distributing security throughout the network space, providing the ability to collect and correlate data from multiple points, thus enabling behavioral signature detection.

Figure 1. Server sink flow types by hour of the week.



Project Goals

To further our understanding of behavioral signature evolution, we set out to contribute to one of network security's greatest challenges: the insider threat problem. This problem calls for distributed behavioral signature detection even more than outside attacks do, because the insider generally will not have to bypass a firewall or rely on tools that are sophisticated or noisy on the network since they already have some level of access.

Our intent is to describe the behavior of a threatening insider from the viewpoint of computer network traffic, first as visible at a major access point, and then, as seen across multiple sensors. We apply both adversary modeling and pathway analysis to create our model.

To determine if the insider behavior signature is detectable is another challenge. It is easier for insiders to cloak their actions in what appears to be normal and benign traffic. Understanding what portions of a signature can be used to effectively identify malicious behavior while keeping false-positives low is another goal of this project.

Relevance to LLNL Mission

Cyber security in general, and next-generation approaches that push forward the technology base in particular, are emerging as a major focus of LLNL. In addition to potentially improving the security posture of LLNL and the DOE complex, this work contributes to a new national initiative to transform cyber security to more effectively address the sophisticated threats of today and tomorrow. The specific problem we address in this project, and the

approaches we chose to pursue, draw upon several LLNL core competencies including threat and vulnerability modeling, distributed computing, and network security.

FY2008 Accomplishments and Results

This project resulted in two overarching "lessons learned."

First, pathway analysis is not particularly effective for computing environments. This is largely because of the sheer number of paths from the outside of a network to an attractive target. We were able to address this by effectively collapsing multiple paths based on equivalent security posture characteristics. However, unlike the physical world where pathways are fairly static, the networked world presents new and changing pathways all the time. This dynamism makes cyber security difficult and pathway analysis results age-off too quickly to be effective.

Second, attempting to detect an insider behavior signature at a single point in time and network space is not feasible. Our studies show that some behavior signatures match up to 80% of firewall traffic in an open-science computing environment.

However, there may be hope. Adding just one more detection point, and correlating the two, reduced the hit rate significantly. We hypothesize that this reduction rate would continue, possibly exponentially, as additional detection points are added. Many factors would have to be considered, such as the ability to do precise time and actor correlation, and the utility of the data being correlated. Also, our project addressed only static behavior signatures; more sophisticated methods of building and detecting dynamic signatures are areas of research that would greatly enhance these approaches to cyber security and the insider threat problem.

In addition to these lessons learned, we made numerous recommendations to the security staff for the network analyzed, to enhance security posture and improve potential for detection of malicious activity.

Figures 1 through 3 are representative of our results.

Related Reference

Wright, C., *et al.*, "On Inferring Application Protocol Behaviors in Encrypted Network Traffic," *Journal of Machine Learning Research*, **7**, pp. 2745–2769, December 2006.

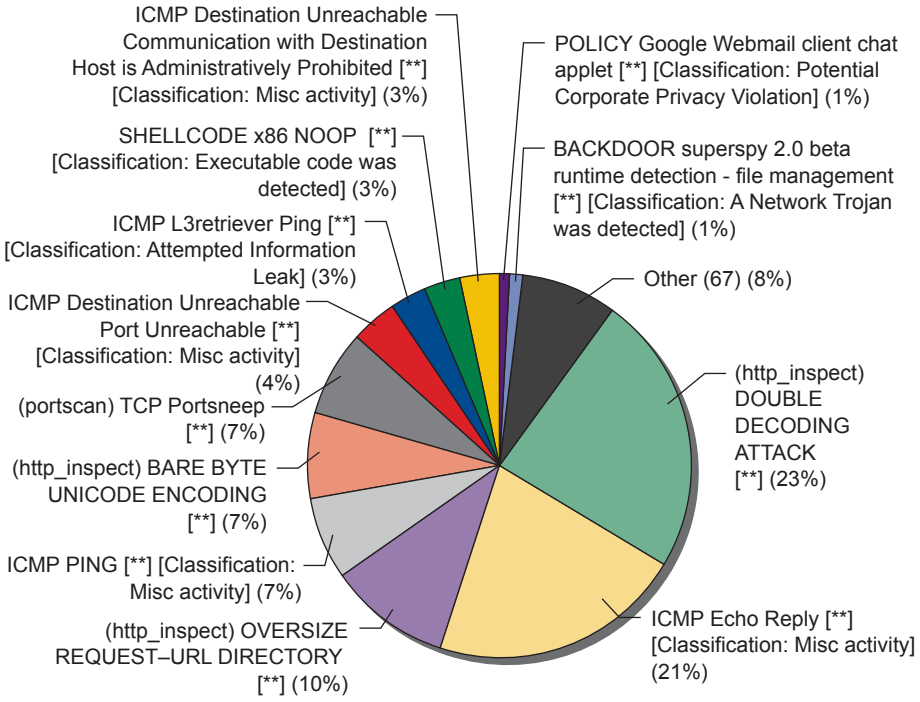


Figure 2. Pie chart depicting SNORT rule alert types at the firewall. (SNORT is a rule-based intrusion detection/prevention system and is the *de facto* standard tool.)

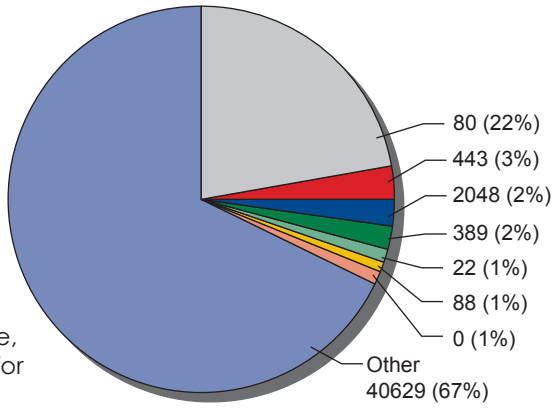


Figure 3. Pie chart depicting the destination port of incoming network traffic. Port 80, for example, is the standard port used for web traffic.